



## Twisting Goppa Codes

Majid Farhadi, Marc Perret

### ► To cite this version:

Majid Farhadi, Marc Perret. Twisting Goppa Codes. Finite Fields and Their Applications, 2008, 14, pp.1091-1100. hal-00967397

**HAL Id: hal-00967397**

**<https://hal.science/hal-00967397>**

Submitted on 8 Apr 2014

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# TWISTING GEOMETRIC CODES

MAJID FARHADI\*, MARC PERRET\*\*

ABSTRACT. The aim of this paper is to explain how, starting from a Goppa code  $C(X, G, P_1, \dots, P_n)$  and a cyclic covering  $\pi : Y \rightarrow X$  of degree  $m$ , one can twist the initial code to another one  $C(X, G + D_\chi, P_1, \dots, P_n)$ , where  $D_\chi$  is a non-principal degree 0 divisor on  $X$  associated to a character  $\chi$  of  $\text{Gal}(Y/X)$ , in the hope that  $\ell_X(G + D_\chi) > \ell_X(G)$ . We give, using a MAGMA program, several examples where this occurs, and where both the initial and twisted codes have same minimum distance, so that initial codes have been improved.

## INTRODUCTION

Let  $X$  be a smooth, projective and irreducible genus  $g$  curve defined over a finite field  $K = \mathbb{F}_q$  with rational function field  $K(X)$ . If  $G$  is a rational divisor on  $X$ , then the Riemann-Roch space  $L_X(G)$  is defined by

$$L_X(G) = \{f \in K(X)^* \mid \text{div}(f) + G \succeq 0\} \bigcup \{0\}.$$

This is a finite dimensional  $K$ -vector space, whose dimension  $\ell_X(G)$  is given by *Riemann-Roch Theorem* :

$$\ell_X(G) - \ell_X(K_X - G) = \deg G + 1 - g$$

where  $K_X$  is a canonical divisor of  $X$ .

Now, if  $P_1, \dots, P_n$  are  $n$  rational points on  $X$  prime to  $G$ , Goppa have defined the *geometric code*  $C(X, G, P_1, \dots, P_n)$  as the image of the map

$$\begin{aligned} \alpha_G : L_X(G) &\longrightarrow \mathbb{F}_q^n \\ f &\mapsto (f(P_1), \dots, f(P_n)). \end{aligned}$$

He then proved the following well-known theorem (see for instance [?], [?], [?] or [?]).

**Theorem** (Goppa, 1981) *If  $\deg G < n$ , then the parameters  $[n, k, d]$  of  $C(X, G, P_1, \dots, P_n)$  satisfies :*

- (i)  $k = \ell_X(G) \geq \deg G + 1 - g$ ;
- (ii)  $d \geq d_G^* = n - \deg G$ .

In this theorem,  $d_G^* := n - \deg G$  is called the *designed minimum distance* of  $C(X, G, P_1, \dots, P_n)$ , while  $d$  is its *true minimum distance*.

Regarding the dimension  $k$  of  $C(X, G, P_1, \dots, P_n)$ , it is well known that if  $\deg G > 2g - 2$ , then  $\ell_X(K_X - G)$  vanishes, so that  $k = \ell_X(G) = \deg G + 1 - g$  is exactly known *and depends only on  $\deg G$* .

---

1991 *Mathematics Subject Classification.* 11G20; 11T71; 14H05.

*Key words and phrases.* Goppa codes.

On the other hand, if  $\deg G \leq 2g - 2$ , then  $\ell_X(K_X - G)$  in general doesn't vanishes, and the dimension  $k$  is only lower bounded by what can be called the *designed dimension*  $k_G^* := \deg G + 1 - g$ . We will take advantage in this paper from the fact that if  $\pi : Y \rightarrow X$  is -say for simplicity in the whole of this paper- a cyclic morphism from another smooth projective irreducible curve  $Y$  defined over  $K$  to  $X$ , then one can build, for any non-trivial character  $\chi$  of the Galois group  $\Gamma = G(Y/X)$ , a *non-principal degree zero divisor*  $D_\chi$  (see Proposition ??). Then, the hope is that  $\ell_X(G + D_\chi) > \ell_X(G)$ , so that the dimension of  $C(X, G, P_1, \dots, P_n)$  is strictly less than the *twisted code*  $C(X, G + D_\chi, P_1, \dots, P_n)$  one's. If moreover the *true* minimum distance of the latter is greater or equal than the former's one, then the initial code  $C(X, G, P_1, \dots, P_n)$  will be improved by its *twist by*  $\chi$ .

In a first section, which is a specialization in the cyclic case of results on representation theory on riemann-roch spaces, we give the construction of the divisor  $D_\chi$ . In a second one, we will give a MAGMA program, and some examples of codes  $C(X, G, P_1, \dots, P_n)$  where this method works.

The authors would like to express deep gratitude to Emmanuel Hallouin and Niels Borne, whose guidance and support were crucial for the successful completion of this work.

## 1. ACTION OF CYCLIC GALOIS GROUP ON SOME RIEMANN-ROCH SPACES

**1.1. Introduction.** Let  $X$  and  $Y$  be two irreducible projective smooth curves defined over the finite field  $K = \mathbb{F}_q$  and  $G$  be a rational divisor on  $X$ . Let  $\pi : Y \rightarrow X$  be a Galois morphism with Galois group  $\Gamma = \text{Gal}(Y/X)$ . Then,  $\Gamma$  acts on  $K(Y)$  by  $\gamma.f := f \circ \gamma^{-1}$  for  $\gamma \in \Gamma$  and  $f \in K(Y)$ . It also acts on  $\text{Div}(Y)$  by

$$\gamma(\sum_P d_P P) := \sum_P d_P \gamma(P).$$

Hence,  $\gamma$  acts on  $L_Y(G_Y)$  for any  $\Gamma$ -invariant divisor of  $Y$ . In particular, for any rational divisor  $G$  on  $X$ , the divisor  $\pi^*(G)$  on  $Y$  is Galois invariant, so that  $\Gamma$  acts on  $L_Y(\pi^*(G))$ .

For the sake of simplicity, suppose from now on, and in the whole of this paper, that :

- (i)  $\Gamma$  is cyclic of order  $m$  ;
- (ii)  $m$  divides  $q - 1$ .

It follows from (ii) that  $K$  contains all the  $m$ -th roots of unity and the characteristic  $p$  of  $k$  is prime to  $m$ . Under these assumptions, elementary reduction theory of matrices implies that there is a canonical decomposition of  $L_Y(\pi^*(G))$  as a direct sum over the characters of  $\Gamma$  of eigenspaces (or isotrope subspaces) :

$$L_Y(\pi^*(G)) = \sum_{\chi} L_Y(\pi^*(G))_{\chi},$$

where, for any character  $\chi \in \hat{\Gamma} := \text{Hom}(\Gamma, \mu_m(K))$ , we denote by  $L_Y(\pi^*(G))_{\chi}$  the subspace

$$L_Y(\pi^*(G))_{\chi} := \{f \in L_Y(\pi^*(G)); \gamma.f = \chi(\gamma)f \text{ for any } \gamma \in \Gamma\}.$$

**1.2. The trivial character.** Of course, the invariant subspace  $L_Y(\pi^*(G))^\Gamma$  is nothing else than  $L_Y(\pi^*(G))_{\chi_1}$  for the trivial character  $\chi_1$ . The following lemma is well known.

**Lemma 1.2.1.**  $\pi^*$  induces an isomorphism  $L_X(G) \rightarrow L_Y(\pi^*G)_{\chi_1}$ .

*Proof.* Let

$$\pi^* : L_X(G) \rightarrow L_Y(\pi^*G)$$

$$f \mapsto f \circ \pi.$$

Then  $\pi^*$  is a linear injective function, for if  $f \circ \pi = 0$ , then  $f = 0$  since  $\pi$  is onto. Moreover, for  $f \in K(Y)$  and  $\gamma \in \Gamma$ , one has  $\gamma \cdot (\pi^* f) = (\pi^* f) \circ \gamma^{-1} = f \circ \pi \circ \gamma^{-1} = f \circ \pi = \pi^* f$  since  $\pi \circ \gamma^{-1} = \pi$ . Consequently,  $\pi^* : L_X(G) \hookrightarrow L_Y(\pi^*G)_{\chi_1}$ . Now, if  $g \in L_Y(\pi^*G)_{\chi_1}$ , then  $\gamma(g) = g$  for  $\gamma \in \Gamma$ , so that for any  $Q \in Y$ , we have  $g \circ \gamma^{-1}(Q) = g(Q)$ . Hence there exists  $f \in K(X)$  such that  $g = f \circ \pi = \pi^*(f)$ . At last,  $(g) \geq -\pi^*G$  implies  $(f) \geq -G$ .  $\square$

### 1.3. Twisting divisors.

**Lemma 1.3.1.** Let  $\pi : Y \rightarrow X$  be a morphism with Galois Group  $\Gamma = \mathbb{Z}/m\mathbb{Z}$ . Suppose  $\mu_m(K) \subset K$ . Let  $\chi \in \widehat{\Gamma}$ . Then there exists  $f_\chi \in K(Y)^*$ , such that  $\gamma \cdot f_\chi = \chi(\gamma) f_\chi$  for any  $\gamma \in \Gamma$ .

*Proof.* We have :

$$1 \rightarrow \mu_m(K) \hookrightarrow K(Y)^* \rightarrow (K(Y)^*)^m \rightarrow 1.$$

We know that  $H^0(\Gamma, A) = A^\Gamma$ . So we obtain, using Hilbert 90 theorem :

$$1 \rightarrow \mu_m(K)^\Gamma \rightarrow (K(Y)^*)^\Gamma \rightarrow ((K(Y)^*)^m)^\Gamma \rightarrow H^1(\Gamma, \mu_m(K)) \rightarrow H^1(\Gamma, K(Y)^*) = 1.$$

By definition of  $\Gamma$  and Galois theory, we have :

$$1 \rightarrow \mu_m(K) \rightarrow K(X)^* \rightarrow ((K(Y)^*)^m)^\Gamma \rightarrow \text{Hom}(\Gamma, \mu_m(K)) = \widehat{\Gamma} \rightarrow 1.$$

Thus the connecting morphism is onto.

Now, let  $g = f^m \in ((K(Y)^*)^m)^\Gamma$ . The connecting morphism  $(K(Y)^*)^m \rightarrow \widehat{\Gamma}$  is defined by

$$(1.3.1) \quad \delta(g)(\gamma) := \frac{\gamma \cdot f}{f}$$

for any  $\gamma \in \Gamma$ . Since  $\delta$  is onto, for a given  $\chi \in \widehat{\Gamma}$ , there exists  $g_\chi = f_\chi^m \in ((K(Y)^*)^m)^\Gamma$  such that

$$(1.3.2) \quad \chi = \delta(g_\chi).$$

Thus ?? and ?? altogether imply :

$$(1.3.3) \quad \forall \chi \in \widehat{\Gamma}, \exists f_\chi \in K(Y)^*, \forall \gamma \in \Gamma, \chi(\gamma) = \frac{\gamma \cdot f_\chi}{f_\chi},$$

which was to be proved.  $\square$

*Remark 1.3.2.* Let  $\pi : Y \rightarrow X$  be a morphism of degree  $m$ . We consider  $\Gamma = \mathbb{Z}/m\mathbb{Z} = \langle \sigma \rangle$ . Let  $\chi$  be a character of  $\Gamma$ . We look for an *explicit* rational function  $f_\chi \in K(Y)^*$ , such that  $\sigma.f_\chi = \chi(\sigma)f_\chi$ . Let  $\zeta = \chi(\sigma)$ . This is an  $m$ -th root of 1 in  $K$ . Let  $f_0 \in K(Y)$  be such that  $f_0 \notin K(X)$ . We can assume that  $\sigma.f_0 \neq \zeta f_0$  (otherwise  $f_\chi = f_0$  works.) We define  $f := \sum_{i=0}^{m-1} \zeta^i \sigma^{m-i} f_0$ . Then  $\sigma.f = \sum_{i=0}^{m-1} \zeta^i \sigma^{m-i+1} f_0 = \zeta f$ , thus  $f = f_\chi$  works if it does not vanish.

Recall that, as is well known, the map

$$\pi^* : \text{Div}(X) \rightarrow \text{Div}(Y)^\Gamma$$

is an injective morphism. Moreover, if  $D_Y \in \text{Div}(Y)^\Gamma$  has disjoint support with the ramification locus  $\text{Ram}(\pi)$  of  $\pi$ , then there exists  $D_X \in \text{Div}(X)$ , such that  $D_Y = \pi^*(D_X)$ . From now on,  $|D|$  will denote the support of a divisor  $D$ .

**Lemma 1.3.3.** *In the situation of Lemma ?? and if  $|f_\chi| \cap |\text{Ram}(\pi)| = \emptyset$ , there exists a unique divisor  $D_\chi \in \text{Div}(X)$  such that the principal divisor  $(f_\chi)$  on  $Y$  satisfies  $(f_\chi) = \pi^* D_\chi$ . We have  $D_\chi = \frac{1}{\#\Gamma} \pi_* (f_\chi)$ .*

*Proof.* Since  $\gamma.f_\chi = \chi(\gamma)f_\chi$ , one has on divisors

$$\gamma.(f_\chi) = (f_\chi), \text{ i.e.}$$

$$(f_\chi) \in (\text{Div} Y)^\Gamma.$$

But  $|f_\chi|$  is prime to  $|\text{Ram}(\pi)|$  by assumption, so that there exists a unique divisor  $D_\chi \in \text{Div} X$  such that  $(f_\chi) = \pi^* D_\chi$ .

Now,  $\pi^* D_\chi = (f_\chi)$  implies  $\#\Gamma.D_\chi = \pi_* \pi^* D_\chi = \pi_*(f_\chi)$ , thus the last assertion holds.  $\square$

*Remark 1.3.4.* If one changes  $f_\chi$  to another  $f'_\chi$ , then  $D_\chi$  changes to another  $D'_\chi$ , such that  $\pi^*(D_\chi - D'_\chi) = (f_\chi/f'_\chi)$  is a principal divisor on  $Y$ . In general,  $D_\chi - D'_\chi$  itself will not be principal on  $X$ , although it will be of order  $m$  in the jacobian of  $X$  since  $m(D_\chi - D'_\chi) = \pi_* \circ \pi^*(D_\chi - D'_\chi) = \pi_*(f_\chi/f'_\chi)$ .

**Proposition 1.3.5.** *Let  $\pi : Y \rightarrow X$  be a cyclic morphism with Galois group  $\Gamma \neq 1$ . Let  $\chi$  be a non trivial character of  $\Gamma$  such that  $|f_\chi| \cap |\text{Ram}(\pi)| = \emptyset$ . Then the divisor  $D_\chi$  of Lemma ?? is not a principal divisor on  $X$ .*

*Proof.* The long exact sequence of cohomology associated to following short exact sequence

$$1 \rightarrow K^* \rightarrow K(Y)^* \rightarrow P(Y) \rightarrow 1,$$

where  $P(Y)$  denotes the group of the principal divisors of  $Y$ , is :

$$1 \rightarrow K^* \rightarrow (K(Y)^*)^\Gamma = K(X)^* \rightarrow P(Y)^\Gamma \rightarrow \text{Hom}(\Gamma, K^*) \rightarrow H^1(\Gamma, K(Y)^*) = 1$$

i.e.

$$1 \rightarrow P(X) \rightarrow P(Y)^\Gamma \rightarrow \widehat{\Gamma} \rightarrow 1,$$

where the middle first map is  $\pi^*$  and the second one is the connecting morphism  $\Delta$ . Now, the defining relation of  $f_\chi$  given in Lemma ?? implies that for the principal divisor  $(f_\chi)$ , one has  $(f_\chi) \in P(Y)^\Gamma$ . Equality ?? means that  $\Delta((f_\chi)) = \chi$ . It follows that if  $\chi \neq 1$  in  $\widehat{\Gamma}$ , then  $\pi^* D_\chi = (f_\chi) \notin \text{Ker} \Delta = \text{Im} \pi^*$ , which means that  $D_\chi \notin P(X)$ .  $\square$

**Proposition 1.3.6.** *With the notations and assumptions of Lemma ?? and Proposition ??, we have*

$$L_Y(\pi^*G)_\chi \simeq (L_Y(\pi^*G + (f_\chi)))^\Gamma.$$

*Proof.* Let

$$\begin{aligned} \phi : (L_Y(\pi^*G + (f_\chi)))^\Gamma &\rightarrow L_Y(\pi^*G)_\chi \\ g &\mapsto \phi(g) = gf_\chi. \end{aligned}$$

We know that

$$(1.3.4) \quad L_Y(\pi^*G)_\chi = \{f \in L_Y(\pi^*G) \mid \forall \gamma \in \Gamma, \gamma \cdot f = \chi(\gamma)f\},$$

and that

$$(1.3.5) \quad (L_Y(\pi^*G + (f_\chi)))^\Gamma = \{g \in L_Y(\pi^*G + (f_\chi)) \mid \forall \gamma \in \Gamma, \gamma \cdot g = g\}.$$

We conclude from ?? and Lemma ?? that  $\gamma \cdot (gf_\chi) = (\gamma \cdot g)(\gamma \cdot f_\chi) = \chi(\gamma)gf_\chi$  so  $\phi(g)$  lies in  $L_Y(\pi^*G)_\chi$ . In order to prove that  $\phi$  is onto, let  $f \in L_Y(\pi^*G)_\chi$ . We consider  $g = ff_\chi^{-1}$ . We have to check that  $gf_\chi^{-1} \in (L_Y(\pi^*G + (f_\chi)))^\Gamma$ . Indeed, we know that for  $\gamma \in \Gamma$ , we have  $\gamma \cdot (ff_\chi^{-1}) = (\gamma \cdot f)(\gamma \cdot f_\chi^{-1}) = \chi(\gamma)f\chi(\gamma)^{-1}f_\chi^{-1} = ff_\chi^{-1}$ , hence  $\phi$  is onto.  $\square$

**Proposition 1.3.7.** *(E.Kani 1986 [?]) If  $E \in \text{Div}(Y)^\Gamma$  and  $|E| \cap |\text{Ram}(\pi)| = \emptyset$ , then*

$$L_Y(E)^\Gamma \simeq f_\chi \cdot \pi^* L_X([\frac{1}{\text{card}\Gamma} \pi_*(E + (f_\chi))])$$

where  $[x]$  denotes the integer part of real number  $x$ .

**Corollary 1.3.8.**  *$\pi^*$  induces an isomorphism  $L_X(G + D_\chi) \rightarrow L_Y(\pi^*G)_\chi$ .*

*Proof.* Using Proposition ??,  $L_Y(\pi^*G)_\chi \simeq (L_Y(\pi^*G + (f_\chi)))^\Gamma$ . With Proposition ??, we obtain  $L_Y(\pi^*G + (f_\chi))^\Gamma \simeq L_X([\frac{1}{\text{card}\Gamma} \pi_*(G + D_\chi)]) = L_X(G + D_\chi)$   $\square$

## 2. EXPLICIT EXAMPLES OF IMPROVED CODES

### 2.1. The hope.

**Definition 2.1.1.** If  $C = C(X, G, P_1, \dots, P_n)$  is a Goppa code, if  $\pi : Y \rightarrow X$  is a cyclic covering of degree  $m$  and  $\chi \in \hat{\Gamma}$ , we call  $C_\chi := C(X, G + D_\chi, P_1, \dots, P_n)$  the *twist* of  $C$  by the character  $\chi$ .

The hope is the following. Let  $C = C(X, G, P_1, \dots, P_n)$  be a given Goppa code over  $\mathbb{F}_q$ , and  $\pi : Y \rightarrow X$  be a cyclic covering of degree  $m$ , where  $m$  divides  $q - 1$ . Then  $L_Y(\pi^*(G))$  is a representation of  $\Gamma$ , which is non-free in general if  $\deg G \leq 2g - 2$ , which means that all isotypic components have not the same dimension. Hence, we can expect that the dimension of the isotypic component for the trivial character, which is  $L_X(G)$  by lemma ??, is not the greater one. We will see that this hope is not always realized, for instance for the canonical divisor (see the remark ??). However, it is sometimes realized, as shown by the examples given in the following subsections. If this hope is achieved for a non-trivial character  $\chi$ , namely if  $\dim L_Y(\pi^*(G))_\chi > \dim L_Y(\pi^*(G))_{\chi_1} = \ell_X(G)$ , and if we are lucky enough for the minimum distance of  $C_\chi$  to be at least equal to  $C$  one, then the initial code  $C$  will be improved by its twist  $C_\chi$ .

**2.2. A family of unramified cyclic coverings.** We will present here an example which may be well known. It has been given at least in [?] with others assumptions on the parameters and with another point of view.

Let  $n \geq 2$  be any integer,  $q$  a power of a prime number, and let  $m = n^2 - n + 1$ . We consider the degree  $m$  Fermat curve

$$F_m : u^m + v^m + w^m = 0.$$

Suppose that  $m$  divides  $q - 1$ , so that  $\mathbb{F}_q$  contains a primitive  $m$ -th root of unity  $\zeta$ . Then the cyclic group  $\Gamma = \langle \sigma \rangle \simeq \mathbb{Z}/m\mathbb{Z}$  acts on  $F_m$  by

$$\sigma([u, v, w]) = [u, \zeta v, \zeta^n w].$$

It is easily seen that this action has no fixed points on  $F_m$ , so that the quotient morphism from  $F_m$  to  $F_m/\Gamma$  is cyclic unramified of degree  $m$ .

Now, consider the curve

$$X : x^n y + y^n z + z^n x = 0,$$

which is smooth if  $m$  is prime to  $q$ , in particular under our assumption that  $m$  divides  $q - 1$ . Since  $n$  and  $m$  are related by  $m = n^2 - n + 1$ , there is a morphism  $\pi : F_m \rightarrow X$  given by

$$\pi([u, v, w]) = [u^n w, v^n u, w^n v].$$

We have

$$\begin{aligned} \pi(\sigma([u, v, w])) &= \pi([u, \zeta v, \zeta^n w]) \\ &= [\zeta^n u^n w, \zeta^n v^n u, \zeta^{n^2+1} w^n v] \\ &= [\zeta^n u^n w, \zeta^n v^n u, \zeta^{n+m} w^n v] \\ &= \pi([u, v, w]) \end{aligned}$$

since  $n^2 + 1 = n + m \equiv n \pmod{m}$ . Hence,  $\pi$ , which have degree  $m$ , factorizes through the quotient morphism  $F_m \rightarrow F_m/\Gamma$ , which is also of degree  $m$ . We conclude that  $X = F_m/\Gamma$ , hence  $\pi$  is cyclic unramified of degree  $m$ , under the only assumption that  $m$  divides  $q - 1$ .

In the following subsections, we will give explicit examples using a MAGMA program where our hope is satisfied for some values of  $n$ ,  $m$  and  $q$ . In all these examples,  $\omega$  will be a primitive element on  $\mathbb{F}_q^*$ .

**2.3. The MAGMA program.** Here is the MAGMA program used for the following computations. The user should enter by hand the parameter  $n$  of example ??, the size  $q$  of the alphabet, the length (denoted here by  $\ell$ ) of the code and the function  $f_0$  of remark ??

```
(//Declaration of the parameters).
n:=??;
m:=n^2-n+1;
q:=??;
assert(IsDivisibleBy(q-1,m));
(//length of code)
l:=??;
t:=(q-1)div m;

(//Declaration of the curves).
k<w>:=GF(q);
```

```

P2 < x, y, z >:= ProjectiveSpace(k, 2);

  (//Declaration of the morphism).
f := x^n * y + y^n * z + x * z^n;
h := y^m + z^m + x^m;
X := Curve(P2, f);
F_m := Curve(P2, h);
F_{F_m} < a, b >:= FunctionField(F_m);
g_X := Genus(X);
π := map < F_m -> X[[x^n * z, x * y^n, y * z^n]] >;
ζ := w^t;

  (//Declaration of f_0).
f_0 := ??;

  (//Declaration of the character χ)
σ := map < F_m -> F_m[[x, ζ * y, ζ^n * z]] >;
for k := 1 to m do
  F_{F_m} < a, b >:= FunctionField(F_m);
  if Pullback(σ, f_0) eq ζ^k * f_0 then
    f_χ := f_0;
  else;
    f_χ := f_0;
  for j := 1 to m - 1 do
    f_χ := f_χ + ζ^{k+j} * Pullback(σ^{m-j}, f);
  end for;
end if;
if f_χ ne 0 then

  (//Declaration of the twisted divisor D_χ)
D := Divisor(F_m, f_χ);
E := Pushforward(π, D);
D_χ := Quotrem(E, m);

  (//Declaration of G).
for n := 1 to 2 * g_X - 2 do
  p := X![0, 1, 0];
  P1 := Place(p);
  G := n * (DivisorGroup(X) ! P1); G_χ := G + D_χ;
  if Dimension(G_χ) gt Dimension(G) then
    repeat
      B_X := Places(X, 1);
      T := Support(G) cat Support(G_χ);
      for j := 1 to card(T) do
        P2 := Random(T);
        B_X := Exclude(B_X, P2);
        T := Exclude(T, P2);
      end for;
    until
  end if;
end for;
χ

```



```

endfor;
for s := 1 to card (BX) - l do
  BX := Exclude(BX, P2);
end for;

(// Construction of the initial code C and the twisted code Cχ)
C := AlgebraicGeometricCode(BX, G);
Cχ := AlgebraicGeometricCode(BX, Gχ);

(// comparison of the parameters).
until MinimumDistance(C) le MinimumDistance(Cχ);
C, Divisor(C);
Cχ, Divisor(Cχ);
end if; end for; end if; end for;

```

**2.4. Example using a cyclic unramified 7-coverings with  $q = 8$ .** Here, we consider the case  $n = 3$ ,  $m = 7$  and  $q = 8$ . We have  $F_m := u^7 + v^7 + w^7$  and  $X := x^3y + y^3z + xz^3$ . In this case  $g_X = m - 3 + 2/2 = 3$ .

We can improve a  $[6, 2, 4]$  code to a  $[6, 3, 4]$  one as follows. With the help of the above MAGMA program, we get the  $[6, 2, 4]$  Goppa code  $C$  over  $GF(8)$  whose generator matrix is  $\begin{pmatrix} 1 & 1 & 0 & 0 & w & w \\ 0 & 0 & 1 & 1 & w^3 & w^3 \end{pmatrix}$  obtained with the divisor  $G = 4(0 : 1 : 0)$ . With the choice  $f_0 = ab^3$ , which gives

$$D_\chi = P + 3Q - 4R$$

where  $P = (0 : 0 : 1)$ ,  $Q = (1, 0, 0)$  and  $R := (0 : 1 : 0)$ ,  $C$  is improved to the Goppa code  $C_\chi$  for the divisor  $G_\chi = G + D_\chi = (1 : 0 : 0) + 3(1 : 0 : 0)$ , whose generator matrix is  $\begin{pmatrix} 1 & 0 & 0 & w^4 & w^5 & w \\ 0 & 1 & 0 & w^4 & w & w^5 \\ 0 & 0 & 1 & 1 & w^2 & w^2 \end{pmatrix}$ . This is a  $[6, 3, 4]$  Goppa MDS code over  $GF(8)$ .

**2.5. Example using a cyclic unramified 13-coverings with  $q = 27$ .** Here, we consider the case  $n = 4$ ,  $m = 13$  and  $q = 27$ . We have  $F_m := u^{13} + v^{13} + w^{13}$  and  $X := x^4y + y^4z + xz^4$ . In this case  $g_X = m - 3 + 2/2 = 6$ . We choose  $f_0 = b^2$  in  $F_{F_{13}} < a, b >$  where  $F_{F_{13}}$  is a function field of  $F_{13}$ . MAGMA gives a  $[8, 5, 3]$  code  $C$ , with divisor  $G = 10(0 : 1 : 0)$ , improved by a MDS  $[8, 6, 3]$  twist  $C_\chi$  with divisor  $G_\chi = G + D_\chi = 8(0 : 1 : 0) + 2(1 : 0 : 0)$ . Here,  $D_\chi = 2(1 : 0 : 0) - 2(0 : 1 : 0)$ . The initial code and twisted one have generator matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & w^{22} & w^4 & w^4 \\ 0 & 1 & 0 & 0 & 0 & 2 & w^{16} & w^2 \\ 0 & 0 & 1 & 0 & 0 & w^{22} & w^{15} & w^{14} \\ 0 & 0 & 0 & 1 & 0 & w^6 & w^{10} & w^{20} \\ 0 & 0 & 0 & 0 & 1 & w^{17} & w^{17} & w^{17} \end{pmatrix}$$

and

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & w^3 & w^9 \\ 0 & 1 & 0 & 0 & 0 & 0 & w^{16} & w^4 \\ 0 & 0 & 1 & 0 & 0 & 0 & w^{12} & w^{10} \\ 0 & 0 & 0 & 1 & 0 & 0 & w^{19} & w^{18} \\ 0 & 0 & 0 & 0 & 1 & 0 & w^{15} & w^{12} \\ 0 & 0 & 0 & 0 & 0 & 1 & w^{10} & w^{15} \end{pmatrix}$$

respectively.

### 3. SOME REMARKS

**Remark 3.0.1. Rational points on the jacobian of  $X$ .** If the jacobian  $J_X$  contains a rational point of order  $m$ , then it corresponds by class-field theory (see [?]) to a cyclic unramified covering of degree  $m$ .

**Remark 3.0.2. The case of the canonical divisor.** The Goppa code  $C(X, K_X, P_1, \dots, P_n)$  constructed from the canonical divisor  $K_X$  of  $X$  will *never be improved by this method*. Indeed, the classical Riemann-Roch theorem can be stated with a Galois action. We have (see for instance in N.Borne [?]) :

**Theorem 3.0.3** ((Equivariant Riemann-Roch Theorem)[?]). *Let  $X$  and  $Y$  be two curves and  $\pi : Y \rightarrow X$  be an unramified morphism with Galois Group  $\Gamma = \mathbb{Z}/m\mathbb{Z}$ . Let  $\chi$  be the character related to representation of  $\Gamma$ , then for any  $D \in \text{Div}(X)$ ,*

$$\chi(L_Y(\pi^*(D))) - \chi(L_Y(\pi^*(K_X - D))) = (\ell_X(D) - \ell_X(K_X - D))\chi(\mathbb{F}_q[\mathbb{Z}/m\mathbb{Z}])$$

where  $K_X$  is a canonical divisor of  $X$ .

**Remark 3.0.4.** This enables us to determine the representation  $L_Y(\pi^*K_X)$  of  $\Gamma$ . Thanks to Theorem ??, we obtain the following result :

$$\begin{aligned} \chi(L_Y(\pi^*K_X)) - \chi(L_Y(\pi^*(K_X - K_X))) &= \\ (\ell_X(K_X) - \ell_X(K_X - K_X))\chi(\mathbb{F}_q[\mathbb{Z}/m\mathbb{Z}]). \end{aligned}$$

This gives that

$$\chi(L_Y(\pi^*K_X)) = 1 + (g_X - 1)\chi(\mathbb{F}_q[\mathbb{Z}/m\mathbb{Z}]),$$

which means that the left representation is the sum of the trivial representation and of the regular representation  $(g_X - 1)$  times. It follows that for the trivial character,  $\dim L_X(K_X) = \dim L_Y(K_X^*)_{\chi_1} = 1 + g_X - 1 = g_X$ , while for  $\chi \neq \chi_1$ ,  $\dim L_Y(K_X^*)_{\chi} = g_X - 1 < g_X = \dim L_X(K_X)$ .

**Remark 3.0.5.** The equivariant Riemann-Roch theorem stated in the preceding remark implies that, for any Galois covering, all isotypic component have the same dimension if  $L_X(K_X - G)$  vanishes, for instance if  $\deg G > 2g - 2$ . Hence, our method for improving the dimension of Goppa codes can works only if  $\deg G \leq 2g - 2$ , as stated in the introduction.

**Remark 3.0.6.** It would be interesting to study also the non-cyclic Galois case !

**Remark 3.0.7.** Of course, if  $g_X \neq 0$ , then any divisor of the form  $D = P - Q$  is non principal if  $P \neq Q$ , and it may happen that  $\ell(G + P - Q) > \ell(G)$ . In this paper we extend the range of possibilities for the choice of a non principal divisor  $D_X$  for a fixed given  $\pi : Y \rightarrow X$  by variation  $\chi$  and  $f_0$  (see remark ??).

## REFERENCES

- [1] N. Borne.— *Une formule de Riemann-Roch équivariante pour les courbes*, Thèse, Université Bordeaux 1, Janvier 2000.
- [2] A. Garcia, F. Torres.— *On unramified covering of maximal curves*, Proceeding AGCT-10
- [3] V.D. Goppa.— *Geometry and Codes*, in: Mathematics and its Applications, vol 24. Kluwer Academic Publisher, Dordrecht-Boston-London, 1988
- [4] E. Kani.— *The Galois-module structure of the space of holomorphic differentials of a curve*, J. Reine Angew. Math. 367 pp. 187–206, 1986
- [5] G. Lachaud.— *Les codes géométriques de Goppa*, in Séminaire Bourbaki 27 (1984-1985), exposé 641
- [6] J.P. Serre.— *Groupes algébriques et corps de classes*. Hermann, Paris 1959.
- [7] H. Stichtenoth.— *Algebraic function fields and codes*, Springer-Verlag, Berlin, 1993.
- [8] M. Tsfasman, S. Vladut.— *Algebraic-Geometric Codes*, Kluwer, Dordrecht, 1991.

\* AMIR KABIR UNIVERSITY \*\* ÉQUIPE ÉMILE PICARD, INSTITUT DE MATHÉMATIQUES DE TOULOUSE, UMR 5219, UNIVERSITÉ DE TOULOUSE II, 5 ALLÉES ANTONIO MACHADO, 31 058 TOULOUSE CEDEX FRANCE

*E-mail address:* m-farhadi@aut.ac.ir, perret@math.univ-toulouse.fr